==Phrack Inc.==

Volume 0x0e, Issue 0x44, Phile #0x13 of 0x13

|=----------=[International scenes]=----------=|
|=----------=[By Various   ]=----------=|
|=----------=[<various@nsa.gov>]=----------=|

In this issue we are glad to have an amazing scene phile about Korea. You may find that it is a bit different from the usual scene philes, but the content will reward you. The author gives us information that is hard to come by and insight that illuminates widely believed misconceptions about Korea. We also have the second part of the Greek scene phile that covers interesting stories from that country's past. We know that Greece goes through tough times and we hope it will make people reflect on the situation there.

Trying to define what 'a scene' is, it's not unlike trying to define what 'the Underground' is. Perhaps it is that fleeting moment where you feel a connection with something. A connection that transcends physical limitations and relies only on interest and passion for, well, for anything really.

The definition of the word 'scene' has changed quite a lot. Some years ago the word 'scene' had a geographical connotation. That's clearly no longer the case. Scenes are becoming increasingly, and thankfully, untethered from physical boundaries. That's not really something new, but it has changed the way most scenes are organized and operate.

Given that physical boundaries no longer are the central defining factor of scenes, should Phrack continue to publish scene philes of specific countries? Maybe the next logical step is to focus on scenes that are defined by field, topic or interest. Maybe Phrack's 'International Scenes' section should be changed to simply 'Scenes' and present overviews of less known sub-scenes or communities built around specific interests.

Gentle reader, what are your thoughts?

-- The Phrack Staff

Some Stories in Korea

--[1 - Introduction

The Korean Peninsula has been divided into two countries for more than sixty years. With the ideological dispute of left and right wings that must have been one of the biggest reasons, the political, economic, geographic, and military factors also played an important role here. It is true that this division system may be affected by the political, economic, and military purpose of the two Koreas, neighboring countries, and their allies.

This situation has caused many tragedies to the people of two Koreas, and has made a various types of tension factors like forcing North Korea to develop nuclear weapons to keep her system in the changing flow of the world. Unlike the past whose main element of conflicts came from ideological one, some large movements trying to maintain their interests dominate the situation of the peninsula.

Over the past decade, the tension between South Korea and North Korea has been alleviated thanks to the Sunshine Policy during the regime of two progressive governments. However, after the present ruling party representing conservative value took over the regime again, the tension relationship began once again and there were some physical conflicts. It will be almost impossible to get over this situation only with the intention and endeavor of two Koreas, because there are so many stakeholders.

This article will mainly focus on the internet and cyber capabilities of North Korea which seem to be not widely known to people, and some attacks against South Korea. So, this will make some differences from the traditional Phrack scenes. But I think the differences don't come from contents but form.

--[2 - Internet of North Korea

It is said that the internet of North Korea was introduced in the early 1990s. Mainly because of internal political reasons, the internet has been maintained in the form of intranet.

In January 1997, North Korea opened the first web site of hers, kcna.co.jp in Japan and opened dprkorea.com which was for business in February 1999. And then NK opened the web site, silibank.com for international e-mail relay. Interestingly, whois lookup will show you that the e-mail account of Technical Contact of this domain is gmail. It is known to gain access to this e-mail relay system is blocked in South Korea. The service is available only to foreigners who joined the paid membership, and people and companies of NK registered in the system.[1] The e-mail exchange with foreigners are allowed but it is said NK authorities check the contents, so the privacy of information will not be guaranteed.

The internet access from inside of NK to outside is very limited, but the intranet connection built inside of NK is active. In October 2002, the building of intranet network which allows connection from all areas of NK was completed. It is called `Kwangmyoung' and started as a research system

of scientific knowledge materials. It is known that the access to outside using this intranet system is impossible.

However, DPS(Department of Postal Service, `Chesinseong' in Korean) of NK hires and manages internet access lines in Beijing of China for their use. It is possible to connect to outside through this internet line. But it is not freely available to all NK people. There are some people who guess there are special lines dedicated only to Communist Party and its army in addition to this line. But any proven materials or information through the technical identification has not been publicly offered yet.

NK has been expanding her commercial web sites for the sake of economic interests and system propaganda, and most of them use servers located in foreign countries. It seems that the web sites opened in the early 2000s have been changed and even disappeared. This may be because NK got a permission for her to use her national domain `kp' from ICANN(Internet Corporation for Assigned Names and Numbers) on September 11, 2007. NK has been opening additional web sites by using kp and will add more. KCC(Korea Computer Center) was chosen as a NK internet address management authority. It seems that NK will open her internet system to the world when she establishes security system and policy by herself, and can control the internet use of people.

The access to the NK web sites for system propaganda like naenara.com.kp and star.edu.kp is not permitted in South Korea but it is possible for us to gain access by using Tor and proxy servers. Some of web sites operated directly in NK were known in the past, but they were accessible through not domain address system but IP address. However, it is not sure they are operated now or they are accessible only from specific regions.

NK also makes use of SNS services like twitter(@uriminzok) mainly for propagating her system, giving news about NK, and criticizing South Korea.

--[3 - Cyber Capabilities of North Korea

It was the magazine "Shindonga"(November 2005) and `2005 Defense Information Security Conference' that introduced cyber capabilities of NK. A related news article about the conference contains the following part, "The capability of NK hackers is similar to CIA's."[2] But the main parts of this article were introduced without objective data, so they were not supposed to be reliable facts.

NK Intellectual Solidarity which consists of NK defectors having a right-wing inclination insists that the scale of NK cyber hacker troop has been on the increase to the level of 3,000 people.[3] But this is not confirmed by objective data, so the confidence level is very low.

DigitalTimes cited American experts, "NK cultivates more than 100 hackers centering around Pyongyang Automation University(Mirim University in the past) every year, and they have capabilities to hack Pacific Command and U.S. mainland computer systems."[4] We can easily think that the world is connected with internet, so the physical distance between U.S. and NK is not an obstacle at all. If the computer systems of U.S. are not so secure, even novice hackers can compromise them.

In the web site of Nosotek which is "the first western IT venture in NK", we can find the following expression, "software engineers are selected from the mathematics elite and learn programming from the ground-up, such as assembler to C#, but also Linux kernel and Visual Basic macros".[5] From this, we can see indirectly there are outstanding programmers who have talents to be hackers.

In the case of Kim Il-Sung University, students have to take the courses of high mathematics and programming regardless of their majors. The university developed the following software: Intelligent Locker(Hard Disc protection program), Worluf Anti-virus(anti-virus program), SIMNA(simulation and system analysis program), FC 2.0(C++ program development tool). From this, we can know that NK also conducts hacking and security research.[6]

It seems quite natural that we can easily judge there are hacker troops in NK in this kind of network age. NK may cultivate hackers for her defense. But we don't have to overstate or underestimate the capabilities of NK. We should be objective more thoroughly when data is not enough for correct judgment. Rational and reasonable policy making and practice come from objective data and judgement based on it.

NK should also remember that her web sites, servers, and network can be compromised, propagate malicious codes, and be used as intermediates. The more NK opens, the more she will be attacked. The attackers will be an organization or a country for the sake of its political and military purposes, hacker group for hacktivism, and script kiddies for fun.

--[4 - Attacks against South Korea

There were two big attacks against South Korea. One is 7.7 DDoS attack(at first, this attack started against U.S. on July 4, 2009, but led to the attack against South Korea on July 7, so we call this `7.7 DDoS' attack in Korea.). The other is 3.4 DDoS attack on March 4, 2011.

--[4.1 - 7.7 DDoS attack

The first attack of 7.7 DDoS began on July 4, 2009(Independence Day of U.S.) and lasted for two days. The targets of this attack were 26 important web sites of U.S. including Amazon, FAA, NASDAQ, NSA, White House. But from the second attack(July 7 to 8), 13 web sites of Korea were added to the target list. Administration, congress, portal, media, financial institutions were included in the list. At this time, Chinese hackers were suspected to be attackers.

From the third attack(July 8 to 9), there were some changes in the target list, and the existing zombie PCs were not used any more. It seems that the existing zombie PCs were blocked and could be no longer available for the next attack. One of the interesting things is that there were some government organizations which establish measures to defend against attacks and security companies, major portal sites giving e-mail services in the target list. From this time, NK was suspected to have done the attack. At least, some of South Korea's conservatives wished to believe this for their political profits.

The final attack(July 10) ended destroying data of zombie PCs which were infected with malicious code for attacks. However, the attacker was not identified. C&C(Command & Control) servers from numerous countries were used for the attack. At that time, South Korea was not prepared for this kind of big attack. Thus, South Korea couldn't avoid a confusion from the attack for three days.

As a result, this attack made South Korea establish various policies of preparedness against DDoS attack. Some hackers of South Korea designed ways to cure zombie PCs using C&C servers of attackers as well as some ways of counterattack.

--[4.2 - 3.4 DDoS Attack

Almost two years after 7.7 DDoS attack, a similar attack occurred at 10:00

in the morning on March 4, 2011. Like 7.7 DDoS attack, it contained political intentions. But the techniques of attack were more advanced. The targets were mainly the web sites of major national infrastructures of South Korea. The web sites of legislative, judicial, administrative, military, diplomatic, financial organizations, and intelligence agencies, police, portal, transportation, power system were included.

The attacker used HTTP GET Flooding, UDP Flooding, ICMP Flooding, and more than 80% was HTTP GET Flooding. And more than 110,000 zombie PCs and 700 C&C servers from 72 countries were used for attack.[7] The attacker used P2P web sites to spread malicious codes.

After the attacker realized that his attack had been detected(the P2P web sites were known and blocked) through the countermeasure, he added new commands to the malicious codes. This is a different part from the past attack. When new attacks started, the configuration of malicious code was changed, and new files were added. Security experts faced new challenges and needed more time to analyze them. The ending time of attacks was not specified clearly in the configuration file. And the host file of system was modified to prevent the update of anti-virus programs. And encryption techniques were used to disturb analysis.

However, new defense systems which had been established since 7.7 DDoS attack were applied and despite more advanced techniques of attack, the damage decreased. One day before the attack, ASD(AhnLab Smart Defense) system collected malicious codes which would be used for attack and analyzed the code. Through this analysis, the exact time and targets of attack came to be known, and more effective response was possible.

South Korea has already established some important response systems since 7.7 DDoS attack. The typical examples are ASD of AhnLab and DDoS Shield of KISA. As I said, ASD system can detect attack before it occurs by collecting malicious codes and analyzing them. DDoS Shield system detects attacking traffics and relays normal traffics to their destinations and throws away abnormal attacking traffics through DNS record modification. Of course, the cooperation system of various related organizations and security companies was established elaborately. In this respect, these two attacks made South Korea build new defense systems and brought the development of the security industry.

This attack was so political but the attacker didn't reveal his exact base intentions. But it is clear that the attacker wanted to test his techniques of attack and judge the response capabilities of South Korea. The attacker might realize what kinds of things he needs for his next successful attack. Maybe, we can judge the real capabilities of the attacker through the next attack.

--[5 - Who are attackers?

One of the questions which people are curious about is "who are attackers?". This is an important question related with political and military purposes. In conclusion, the judgement through the technical analysis about the question, `who are attackers?' has not been disclosed to the public. In a nutshell, the attacker may be a guy, a group, an organization, or a country that holds its ground against opponents and so has an obvious justification to attack or wants to seize the hegemony of internet world.

For whom are not interested in this kind of general and abstract conclusion, following judgements and the grounds can be given. This is based on a simple presumption, so you'd better not take it too seriously.

The first ground of presumption that NK could be a probable attacker is GNP(Grand National Party) and Chosun Ilbo were included in the attack target list. GNP is the ruling party of South Korea and its philosophical background is based on conservatism, and it is hostile to NK from a political standpoint. Chosun Ilbo is also a leading conservative media and has a hostile point of argument to NK. The contention of Chosun Ilbo has not always been rational and showed us it may manipulate public opinion for its profit. Of course, people of progressive idea are not always friendly to NK without any condition. The fact that these two targets which can be hostile to NK for their political reasons are included in the list makes us guess the attack might be conducted by NK. This judgement came from the special situation of the Korean Peninsula.

The target list of 3.4 DDoS attack contains a particular web site. It is Dcinside, a common community web site. If the attack had been for political purpose, the web site would have had no reason to be in the list. By the way, on January 5, 2011, some posts to blame for NK's leaders were registered in one of NK web site, uriminzokiri.com which the Committee for the Peaceful Reunification of the Fatherland manages to propagate NK's political system. On January 8, 2011, the twitter account of NK(@uriminzok) was compromised and attackers posted some critical comments about NK and the leader Kim Jeong-il, Kim Jeong-eun. Some members of Dcinside insisted they did. After two months later, Dcinside was in the list of target. This is the second ground of presumption.

Police of South Korea presumed the attack of NK because the source IPs of attack might have been DPS's which DPS of NK hires in China. But one police concerned told a press, "It is difficult to make clear the exact entity about the main body of this DDoS attack."[8] This shows us that the judgement of police might not be clear. To ensure a clear evidence, police told the press they would do a cooperative investigation with China police, but the results of any cooperative investigation has not been released yet. Because only small number of people possess some sensitive information, various conspiracies seem to appear.

Some people who think the attack didn't come from NK suggest the followings: if NK had a perfect attack plan and was not an idiot, they would not revealed the IP addresses she hired in China with causing political problems. On the contrary, the third force who is familiar with the tension of two Koreas and want to use this situation for its profit rather conducted the attack.

A lot of detailed technical analysis has been published many times in korea since the two attacks. In the technical documentations and presentations, the experts of South Korea didn't specify the source of the attacks because they are afraid of arbitrary interpretation by some people. South Korea is a divided country and any information can be interpreted arbitrarily by some people depending on their political or ideological purposes. In the white paper, "Ten Days of Rain" of McAfee, we can find this part, "This may have been a test of South Korea's preparedness to mitigate cyber attacks, possibly by North Korea or their sympathizers."[9] This has been quoted mainly by some conservative organizations and medias for their political purposes to confirm the attack of NK.

--[6 - Some prospects

Some phenomena(for example, making zombie PCs regularly) of the preparation for a powerful DDoS attack has been detected. I am not sure this is the extension of the past and conducted by the past attackers. However, if a new attack occurs, the attacker will test new techniques and South Korea

will inspect her defense systems. Of course, South Korea will also be able to have a chance to establish a new defense system and more advanced attack techniques.

South Korea has carried out more than material preparations through the various forms of cyber attacks. This is because South Korea government and companies realized the importance of hackers' help. This started from getting over the wrong awareness about hackers in the past. However, when they looked for good hackers who could help them, they realized that there were not so many hackers as they wanted. So, the need of running programs that can foster good hackers has begun to rise.

About ten years ago, the hackers of South Korea organized communities and hacking teams by themselves, and proceeded various researches and discussions. At that time, they had strong desire for knowledge and pure research, and their findings were shared freely with little thought of money. And they didn't use their knowledge for the purpose of financial crime. But the government and companies considered hackers as criminals. Sometimes, police tried to arrest hackers for their own profits and blocked their activities. In this kind of oppressive situation, hacker had to stop their growth momentarily. Consequently, this led to the retreat of cyber defense capabilities of South Korea. Hackers can't post an exploit code in a web site. Because the related law defines 'hacking' too comprehensively, so it is still illegal to post an exploit code in an open web site in South Korea.

Watching various cyber attacks for the purpose of political and financial reasons around the world, the government and companies of South Korea realized that bringing up hackers is closely linked to the defense of country and profits of companies. So, they run some hacking contests to find good hackers and support some hacking and security clubs of universities. These kinds of action are still not so well formed to the level of systematically perfect process, but these fostering programs are expected to be proceeded in more concrete shape through various cyber attacks.

Of course, the hackers of South Korea have tried to prove the value of their existence and to grow up by themselves without any help of government and companies. For instance, they have participated in the finals of DefCon CTF since 2006. In 2006, 'East Sea'(This refers to the territory of Korea) team went to the final of DefCon CTF and this was the first time for a foreign team to take part in it. And this led to the organization of one team for DefCon CTF which consisted of some members of leading hacking teams of South Korea. This was helpful to correct the wrong awareness of media about hackers. And some hacking and security conferences have been held every year by hackers. Even some hackers take part in the penetration test projects for government. The hackers of South Korea now prove their contribution and existence value through these activities.

There will be two important elections, a general election and a presidential election in South Korea next year. And some political attacks can be expected regardless of the types of attack.If some large-scale attacks occur again next year, some people will likely assert it as a conduct of NK even if it is not by NK. Some politicians of two Koreas fell under suspicion of bringing unrest on the peninsula intentionally to achieve their political goals at the time-sensitive period.

We can easily anticipate various forms of attack to occur continuously if the division state of two Koreas remains, and new strains occur, or if someone or country needs them for profit. Currently, one of the best solutions for this problem is to relieve the political tensions through the

promotion of common interests of surrounding countries of the Korean Peninsula and to achieve the cooperation relationship. The stability of the Korean Peninsula can contribute to the peace of the world as well as East Asia owing to the close connection of countries.

--[7 - References

[1] Seong-jin Hwang, Young-il Gong, Hyun-ki Hong, Sang-ju Park, "Report about Cooperation in Broadcast Communications Between South Korea and North Korea"
[2] http://www.sisaseoul.com/news/quickViewArticleView.html?idxno=1154
[3] http://news.chosun.com/site/data/html_dir/2011/06/01/2011060100834.html
[4] http://www.dt.co.kr/contents.html?article_no=2011070102010251746002
[5] http://www.nosotek.com
[6] Chan-mo Park, "Software Technology Trends of North Korea" http://www.postech.ac.kr/k/univ/president/html/speeches/20030428.html
[7] http://www.ahnlab.com/kr/site/securityinfo/newsletter/magazine.do
[8] http://www.seoul.co.kr/news/newsView.php?id=20110407008034
[9] McAfee, "Ten Days of Rain - Expert analysis of distributed denial-of-service attacks targeting South Korea" http://dok.do/srVOcq

---

What's past is prologue

anonymous underground greek collective - anonymous_gr@phrack.org

----[Introduction

First things first. This is the second part of the previous scene phile on the Greek underground scene [GRS]. Although the primary authors are the same as the first part, this time many people contributed information, stories, facts and even whole paragraphs of text. We were positively surprised by the response and the attitude of the community that decided to help us in order to make this second part better. Hence the new authorship details. Also, the email alias from above is now forwarded to the people that helped.

The truth is that we had a great time receiving irrelevant flames by people who didn't even read the first two paragraphs of our previous scene phile. In a struggle to avoid future unfortunate comments, we would like to stress the fact that we are not capable of talking about every aspect of the Greek scene in just a few paragraphs. In fact, space is not the only problem. Privacy is a fundamental characteristic of all scenes. There are people who don't want to publish or openly talk about their actions, and there are certain stories/facts that we are not aware of. That said, we believe that the following text covers, not all, but a fair amount of the history of the Greek scene. If you don't comprehend the previous sentences, then maybe you should try reading something else. Or maybe try writing/producing something yourself, huh? How about that?

We would also like to remind you that we will once again try to refrain from referring to particular nicknames/handles. We will, instead, give a macroscopic view of our scene's past glory. Btw, you may notice a focus on cities other than Athens. That's a byproduct of the fact that most of the people that provided information are not from Athens.

```
----[ Dawn of time
```

At the dawn of time there were BBSes. And FidoNet.

The very first BBS in Greece, named .ARGOS system, started operating in late 1984. It was a non-networked BBS, mostly built around a message bulletin board. It was arguably the first online community in Greece. Another early BBS was AcroBase established in 1988 [ACR]. The next major event was in 1989 when the first FidoNet nodes in the city of Thessaloniki became active. They connected the Greek BBS community to the world by FidoNet mail and several local and global echomail (usenet news-like) areas. In 1992 Compupress [CPS], a very creative and innovative (for Greek standards ;) publishing company, very famous among Greek computer users, launched its BBS, codenamed "Compulink". 1994 most people agree that it was the "Golden Era" of Greek BBSing. There were around 100 FidoNet nodes in most urban and rural areas of Greece. The "Twilight Zone" BBS was offering public access to a selected choice of usenet groups and public access to Internet email through a UUCP-to-FidoNet gateway. Several regional and some international FidoNet-technology networks other than FidoNET connected most of the amateur computer community in Greece at that time. In Thessaloniki there were weekly FidoNet meetings every Friday, forming the first stable, most widespread and long-lived (till today!) Greek amateur computer society. There were meetings hosting over 30 to 40 people, in times when Computing and Information Technology were terms almost unheard of in Greece. In 1996, the FidoNet nodelist count drops to 51. This was mainly due to the increasing number of ISPs and dialup users, and it was the start of demise for the BBS/FidoNet era of Greece.

Around that time, Compupress' Compulink BBS evolved into a full blown, but tiny, ISP that provided dialup access to the Internetz while at the same time maintaining its BBS service. In 1995-97 the Greek underground was heavily involved in hacking Compulink and its BBS services; there were a lot of incidents and even formal complaints. The fights between Compulink's administrators and well-known members of the underground are almost legendary. This era saw the founding of several hacker (with and without quotes) groups, and is considered by many as the birthplace of the Greek scene.

At this point we should mention that Compupress was the publisher of Pixel, a very famous and influential magazine for personal computers. Pixel first appeared in 1983 and usually included type-in programs as code listings! In 1987, Pixel published the details for one of the oldest virii written by a Greek guy [PIX]. The virus was randomly displaying the message "Program sick error. Call doctor or buy Pixel for cure description". Leet or what?

In the following years, more companies entered the Internet market and Internet access started to spread. Early ISPs were just charging a yearly fee for dial-up access, and each phone call to them costed a small one-time amount (~20 drachmas). These led to a lot of people downloading warez off Usenet, idling on the Greek IRC network (GRNET) and wardialing. The suits of the ISPs and the phone company (OTE) saw that as a cash cow to milk, reacted quickly and established time-based charging (security counter measures? :p). That's the point it started to become expensive for end-users to access the Internet.

This period saw the emergence of a lot of "hacker" groups. This time the quotes are necessary, however there were noteworthy exceptions. Most of these groups focused on attacking the ISPs of the time. In one specific incident, the ISP Hellas On-Line (HOL) was hacked and its main password file was stolen and exchanged in the underground. In order to cover the breach and cause confusion, HOL is rumored to have started distributing a

fake password file among the underground. What needs to be highlighted is that this was one of the first 'dirty or at least "less than sincere" incident response tactics' used by companies as they started to become targets to attacks.

At this time most of the serious hackers were mainly individuals, sometimes organized in anarchy groups that used to have fun breaking things, both metaphorically and literally :) Some day in 1995, #grhack (!= grhack.net) gets established in undernet. #grhack was an IRC room where several skilled people used to hang out and exchange information. #grhack is still so respected among the Greek hackers that several lame Greek cockroaches try to convince one another that they were supposedly active back in the day (fuck off, you know who you are). It was in #grhack that the term "GHS" (Greek Hackers Society - "S" for "Society" and *not* "Scene") first appeared. GHS was exactly what the initials described, a community that consisted of people with respectable and notable skill set and state of mind, people that actually *hacked* (as opposed to the ones whose knowledge is limited to merely running sqlmap and other canned tools).

Additionally, members of #grhack were also the creators of hack.gr and grhack.gr [GGR], two old school sites representing the state of the scene at the time. It's interesting to note that the hack.gr user pages are still up and running at [HGR] (most people listed there are/were respectable, however some idiots also managed to get there). Also, grhack.gr is still maintained by one of the guys (greets and respect)!

Of particular mention was a group of hackers situated mainly (but not strictly) at the city of Patras and associated with hack.gr. They had advanced skills, anarchist ideologies, and weird links with mind-expanding experiences (LSD? Who knows... ;). It is clear that their mentality had a lot to do with their deep education and love of reading (outside technology as well). A couple of them even transcended the borders of Greece and became members of the famous hacking group ADM. Their work was and still is inspirational to a lot of us. It is also worth noting that apart from ADM, members of the Greek underground have participated in or have been founders of other famous hacking groups or communities such as w00w00, ElectronicSouls, el8, 9x, POTS and probably others.

1996-1999 was a high time for the Greek computer underground related press (the traditional mainstream computer press was dominated by the RAM magazine). Several publications surfaced, "Laspi", "The Hack.gr Gazette" and many more. Their focus was primarily on the freedom of speech/information. Some of them were humorous, while others used caustic words to describe, according to the authors, unethical acts of people who got famous by abusing the term "hacking". For example, "Ypokosmos tou Internet" [IUW] (Internet Underworld) was one of the most famous zines, kinda like el8, ZF0 etc ;). Internet Underworld focused on exposing the security and privacy related blunders of ISPs and other poorly maintained organizations/companies without however publishing private data online. It was created in response to the "Kosmos tou Internet" (Internet World), a traditional press magazine. The Internet Underworld zine was shut down by OTE officials who threatened(?) VRnet (their hosting provider) with disconnection. The interested reader can find more details at [ISE] and [TEL], two articles that give more information on the publications of the time (unfortunately they are in Greek but Google Translate is your friend).

In 2001 the first Greek "con" took place in Athens. It was called "HOUMF! Con version 0.0" (Hacking Organisation of Unix Mother Fuckers [HMN]) and it brought together people from the Greek underground with interests in security and hacking [HMF]. Since it was only a "demo" (hence the 0.0

version number :) of a full conference, there were only three talks given [HMT]. However it was considered a huge success since there were about 150 participants, an impressive number if you consider the size of the Greece scene at that (and this really) time. By the end of December 2000, more than 100 people had expressed their interest to attend it!

HOUMF v1.0 was scheduled for the April of 2002. Due to the media going berserk on a new disease spread at the time, the organizers were unable to find a room to host the meeting. Preparations ended abnormally, disappointing a lot of people who would love to attend. It was then when most Greeks did what they knew best; Troll and flame the organizers for no obvious reason. The truth is that there hasn't been any attempt for another underground con in Greece since then. Crappy remarks from worthless people aside, the truth is, if anyone was better at organizing an underground con of this magnitude, they'd just be doing it already.

Around 2000-2001 two more groups appeared in the scene, USF (United Security Force) and UHAGr (United Hackers' Association of Greece). Both were quite active in efnet and undernet, so, several people may recall their names as well as both good and bad memories along with them. It's quite notable that there was an interesting hatred among the members of the two teams, maybe mostly because of personal differences, but looking back in time one can only see the fun part of it. USF and UHAGr both had their own websites; www.infected.gr [INF] and www.uhagr.org [UHA] respectively, where one could see a bunch of releases (papers, codes etc.) as well as funny material, pics from meetings and so on. As far as we know, members of the two teams used to meet in real life in Thessaloniki and Athens in order to have fun and break things.

In 2003-2004, r00thell came into existence. r00thell wasn't a team in the strict sense, it was an active think-tank of 5-6 people mostly interested in exchanging techniques and ideas. One of the most funny things about r00thell was their members' interest to explore exotic architectures which eventually led to a development of a whole heterogeneous network that these guys had access to (AIX, SunOS, HP-UX, etc.). If r00thell had a leader that would be the webmaster of kizoku.r00thell.org, a security portal were one could find interesting texts and several resources. A very interesting 'about' page can be found at [R00], titles of some texts at [R0T] and some projects they used to work on at [ROP].

The same (more or less) people that spawned r00thell, were the creators of other communities as well. Ono-sentai [ONO] was such an example. Ono-sentai was born some time around 2001-2002 and it seems like the members had really fun times. It's unfortunate that the site is written in greeklish; we wish everyone was able to read the sections 'about' and 'kotsanes'! Nevertheless, the website features technical content that may be in value even nowadays (wardialing results, local root exploits, papers and other resources which are worth studying). Apart from the technical content, ono-sentai became very famous for the detailed treatise on the non-existence of Santa-Clause (!) which you can find at [ONS]. We'd love to see an English version of this text; maybe we will some day convince the guy who wrote it to do a proper translation :p For now, you can try Google Translate on it :p

It has always been believed that many members of the Greek underground struggle to mimic the behavior of certain USA groups/communities. We believe this is not an issue specific to our local scene and it's not bad either, at least not by default ;). In the past, several people have tried to follow the principles of pr0j3ct m4yh3m but most of them have failed miserably. Back in 2001, a zine called 'keyhole' started to circulate in the underground. 'Keyhole' was a zine like el8, h0no etc but

only made it to the first issue ;) The zine's authors, calling themselves 'OSS' (Open Secret Society), pretended to be anonymous hackers that exposed people for fun; A few days later, their identities became known. Most people agreed that 'keyhole' was a bad move; as far as we know, no one of the guys being flamed in the zine had hurt the authors.

'Keyhole' was immediately considered an unjustifiable show-off that displeased several members of the Greek underground. It later became obvious that a group of people, named 'CUT' (Ch0wn Unix Terrorists) [CUT], were displeased the most; after managing to identify the 'keyhole' authors, CUT broke into their servers, sniffed mails, IRC logs and other funny material and eventually published a zine called 'asshole' which was considered a reply to 'keyhole' (hence the name). An interesting manifesto [CMN] was also sent to a famous Greek security portal. Although we believe that publishing sensitive private information is unethical, 'asshole' showed the 'keyhole' authors what it feels like to have your ass exposed. In the manifesto, the authors of 'asshole' reacted to all that 'whitehat vs. blackhat' bullshit that had started to affect the Greek communities.

Since that time, more zines have emerged in our local communities usually targeting individuals. Our advice: If you don't like someone, just ignore them :)

To our knowledge, the first arrest in Greece related to computer crime law took place in the September of 2000. It was a surprising and unprecedented move made by the Greek authorities, since prior to this incident there had been only warnings(?) so to say from law enforcement just to scare people off. The CCU (Computer Crime Unit) managed to locate and arrest a student of the Engineering School of Xanthi, who was later charged for causing damage to a very famous Greek ISP. Before this very first arrest, most people in the local hacking communities ignored the presence of intelligence agencies, but this unfortunate event signaled a new era of the Greek underground; an era characterized by an inherent suspicion in members of the underground that even their closest friends could be members of intelligence agencies. Unfortunately, this is a delicate issue which we wouldn't like to discuss further. Many people seem to be involved and we wouldn't like to hurt anyone.

Last but not least, here's a list of other communities that were (or maybe still are) active within the Greek underground:

1. System Halted

2. Ethnic/nationalistic groups (which shall remain unnamed).

----[Demoscene

The demoscene has always been an integral part of the computer underground. A lot of people believe it may be its pure heart nowadays that so many things in rest of the underground scene seem to be corrupted and rotten.

This part of the phile concerns the past of the PC demoscene in Greece. That is not to say that the greek demoscene has been PC-only. Sceners from such platforms as the Amiga, Atari, CPC, C64 and Spectrum have been part of its mosaik. We, however, are going to focus on the PC-specific demoscene.

In the introduction we stressed the fact that we wouldn't like to refer to particular nicknames of the Greek scene. Nevertheless, the demosceners had no problem having their nicknames revealed, so, we thought it would

be nice to give credit where credit is due ;)

As in most cases, one would expect the PC demoscene to have originated from big cities like Athens or Thessaloniki (where over 50% of the country's population is located), but surprisingly that was not the case. The story goes back to 1992 in the town of Katerini, where a group called ASD (Andromeda Software Development) was formed, and started uploading small productions to COSMOS BBS, a local Bulletin Board System. The group in the beginning consisted of Navis and Incus, creating PC utilities, but later Amoivikos joined them, and as a team decided to turn into graphics programming. Although Navis had previously coded various effects in C64 and PC, Cdemo5 should be considered the group's first demo.

Meanwhile, three university students in Athens (Laertis, Jorge and Zeleps), decided to put a group together called Nemesis, but only released one single production in 1994 called spdemo which was an advertisement for a local BBS called Spectrum. It was quite a big thing when Megaverse BBS came online in the city of Patras around 1993. It functioned as a local demo repository, copying demos directly from Future Crew's own Starport BBS in Helsinki and distributing them locally. Dgt, the owner of Megaverse, along with emc, fm, gotcha and nEC, most of them users of a local BBS called Optibase, formed a group called dEUS which was destined to play a big part in the Greek PC demoscene. moT, the group's musician, was finally added to the group, which led to the release of their first production called Anodyne on the 5th of July 1994. dEUS was the first group in Greece to incorporate some kind of design in their demos and the first to submit a production, a 64k intro, to the Assembly Demoparty in Finland, although they never got past the preselection round. More importantly though, they were the first group to organize a demoparty in Greece. This initiative would eventually result to Patras becoming in a way a "capital" for the greek demoscene. The first demoparty that dEUS organized took place on April 28, 1995 in an abandoned bank branch in the center of Patras and was a big success, gathering sceners from all around the country. ASD won the first place in the demo competition with their demo "Counterfactual", marking the beginning of their long winning career. The same year saw the formation of another group. Demaniacs were found in February of 1995 in Xanthi, by Cpc and NeeK, two students at the Democritus University of Thrace, who after watching Second Reality, decided to make something alike on their own, leading to an intro called "pandemonium". Later that year Theo joined them as a musician, leading finally to their first production with sound in March 1996. Gardening 96 took place the following year, this time at the University of Patras' theater, which became the standard location for the parties that followed. The third and last Gardening event took place in 1997 at the same location. At that time, many other groups existed, notably Helix, Debris, Arcadia and Red Power. Little did anyone at that time know it would be the last of The Gardening demoparties. And suddenly, that was it. No demos came out for the following four years, no parties took place, and the scene seemed quite dead. When in the the year 2000 a LAN party, organized by many sceners took place in Athens, it was the closest it could get to a sceners' meeting. However, no productions came out of it.

It was the following year that something significant happened. A demo-dedicated channel was created in GrNet, a greek IRC network, and gathered many of the previously scattered greek sceners as well as new ones. This led to an actual demoparty taking place. Digital Nexus 2001, which took place in Athens, and was organized by cybernoid, apomakros, doomguard and Abishai. ASD won the demo compo once more, presenting "Cadence and Cascade", the first Greek GPU-accelerated demo, which signaled a new era for the Greek demoscene. It is not well known though, that at the same party, Psyche, Raoul and zafos, three students from the

university of Patras, resolved to revive the Gardening demoparties that had taken place at their University a while ago, and to form a demo group, later called nlogn. The fruit of their cooperation was a new demoparty called ReAct, which tried to revive the Gardening atmosphere, and took place on the 19th of April 2002. ASD with aMUSiC, their first musician since the group's formation, won the demo compo with their demo "Edge of Forever". The Greek demoscene seemed to be entering a new era indeed. A few new groups appeared, such as Quadra, The Lab, Psyxes, Nasty Bugs, nlogn and Sense Amok and things for a while looked promising. However, most (if not all) of the newly formed groups never released more than a couple of productions, and never managed to reach the level of productions that were made outside of Greece. Older groups, apart from ASD, never managed to release any new productions. Most of them disbanded but kept coming to parties. ReAct took place in 2002, 2003 and 2004, and then a demoparty called Pixelshow, organized by gaghiel, continued this long running tradition of having a party in the University's theater. Pixelshow took place twice, in 2005 and 2007 (the 2006 event was cancelled), and was the last demoparty to have taken place in Greece so far.

Some things should be added concerning ASD at this point, since their fame is way beyond the Greek demoscene. Although almost no Greek group ever achieved fame outside Greece, ASD is one of the most famous demogroups worldwide. They currently hold the record of scoring four times 1st place in the combined demo compo of the Assembly demoparty, as well as having received eleven scene awards (demoscene's most prestigious award) so far. Their productions are marked by painstaking attention to detail, extremely well crafted transitions that have become their trademark, as well as a progressive metal soundtrack most of the times, composed by aMUSiC and Leviathan, the group's musicians.

----[What's past is prologue

Relax, take a deep breath and try to think what do you want your place to be in the great scope of things. The (Greek) scene will go on with or without you, with or without any one of us. The scene is a collective. Respect it and it will respect you back. Give to it and you will receive. Understand the true spirit of hacking and stop being a Chrysaora Sqlmapis [SUB].

In order to write this article, we contacted several people to ask for information. A lot of people helped not only with information, but also with anecdotes and even actual text. They have our respect and we thank them. Of particular mention are zafos/nlogn and amv/ASD. Also, we respect the fact that some people didn't want to share or have their stories made public, but nonetheless provided helpful feedback. Thank you guys too.

----[References

[GRS] http://phrack.org/issues.html?issue=67&id=16
[ACR] http://www.acrobase.org/
[CPS] http://en.wikipedia.org/wiki/Compupress
[PIX] http://www.f-secure.com/v-descs/pixel.shtml
[GGR] http://www.grhack.gr/ and http://www.grhack.gr/first_page/
[HGR] http://users.hack.gr/
[IUW] http://web.archive.org/web/19990428222240/http://iuworld.vrnet.gr/
[ISE] http://www.isee.gr/issues/01/special/
[TEL] http://www.e-telescope.gr/el/internet-and-computers/
47-online-journalism

```
  [HMF] http://web.archive.org/web/20011020020500/houmf.org/v0.0/
  [HMN] http://web.archive.org/web/20020208000350/
        http://ono-sentai.jp/readkotsanes.php?id=11
  [HMT] http://web.archive.org/web/20011212094327/http://houmf.org/v0.0/
        papers.go
  [INF] http://web.archive.org/web/20011202184457/http://www.infected.gr/
  [UHA] http://web.archive.org/web/20030806115340/http://www.uhagr.org/
  [R00] http://web.archive.org/web/20050220152149/
        http://www.r00thell.org/about/
  [R0T] http://web.archive.org/web/20050220232518/
        http://www.r00thell.org/papers/
  [ROP] http://web.archive.org/web/20031007021404/
        http://r00thell.org/projects.php
  [ONO] http://web.archive.org/web/20020330152233/http://ono-sentai.jp/
  [ONS] http://web.archive.org/web/20020305052051/
        http://ono-sentai.jp/readkotsanes.php?id=3
  [SUB] http://tinyurl.com/882vez7
  [CMN] http://web.archive.org/web/20050218172857/
        http://www.ad2u.gr/mirrors/CUT.txt

        http://web.archive.org/web/20050219114701/
        http://www.ad2u.gr/mirrors/toxicity.email
  [CUT] http://web.archive.org/web/20050206231527/
        http://www.ad2u.gr/article.php?story=20030105175233835


  ----[ EOF
```